DTIC FILE COPY

CSC-EPL-87/004

(2)

NATIONAL COMPUTER SECURITY CENTER

AD-A221 813

FINAL EVALUATION REPORT OF COMPUTER SECURITY CORPORATION SENTINEL

VERSION 3.13

DTIC ELECTE MAY 23 1990 S B D

13 July 1987

Approved For Public Release:
Distribution Unlimited

90 05 23 001

SUB-SYSTEM EVALUATION REPORT

COMPUTER SECURITY CORPORATION

SENTINEL VERSION 3.13

NATIONAL
COMPUTER SECURITY CENTER

9800 SAVAGE ROAD
FORT GEORGE G. MEADE
MARYLAND 20755-6000

July 13, 1987

CSC-EPL-87/004
Library No. S228,516

This page intentionally left blank.

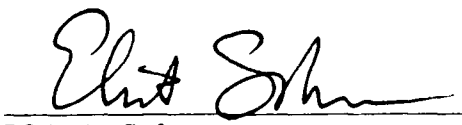
CSC-EPL-87/004
Library No. S228,516

FOREWORD

This publication, the Sub-system Evaluation Report, Computer Security Corporation, Sentinel Version 3.13, is being issued by the National Computer Security Center under the authority of and in accordance with DoD Directive 5215.1, "Computer Security Evaluation Center." The purpose of this report is to document the results of an evaluation of CSC's Sentinel Version 3.13 product. The requirements stated in this report are taken from DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA, dated December 1985.

DTIC
COPY
INSPECTED
4

Approved:



July 13, 1987

Eliot Sohmer
Chief, Product Evaluations and Technical Guidelines
National Computer Security Center

...y Codes
Dist | Avail and/or Special
A-1

ACKNOWLEDGEMENTS

Evaluation Team Members

Joseph Bulger
Leon Neufeld

National Computer Security Center
9800 Savage Road
Fort George G. Meade, Maryland 20755-6000

CONTENTS

This page intentionally left blank.

EXECUTIVE SUMMARY

The Sentinel Security System product has been evaluated by the National Computer Security Center (NCSC). Since Sentinel is considered to be a security sub-system, rather than a complete trusted computer system, it was evaluated against a relevant subset of the requirements in the DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA (Criteria), dated December 1985. The subset for this product includes identification and authentication, discretionary access control, and audit.

The NCSC evaluation team has determined that Sentinel, when configured as tested, is capable of applying these security features to data stored on the non-removable hard disk of an IBM PC/XT(1). Sentinel implements user identification and authentication by requiring each user to enter a valid password, prior to allowing access to the protected machine. Sentinel maintains discretionary access control by mediating all accesses to files (protected objects). Sentinel maintains an audit of user actions during the validation of system and object access

The security mechanisms can be maintained only if both the operating system in which Sentinel runs, and Sentinel's operational files are protected from unauthorized modification. Since Sentinel's protection mechanisms are implemented in single-state machine hardware, it becomes essential that user/system separation be maintained. In systems with this type of architecture, non-privileged users operate in the same memory space as the security-related system functions; hence it would be possible for an experienced user to modify the operating system and circumvent the security mechanisms without the likelihood of detection.

---

(1) IBM PC, PC/XT, PC/AT are registered trademarks of International Business Machines Corporation.

This page intentionally left blank.

INTRODUCTION

Background

On January 2, 1981, the Director of the National Security Agency was assigned the responsibility for increasing the use of trusted computer security products within the Department of Defense. As a result, the DoD Computer Security Center was established at the National Security Agency. Its official charter is contained in DoD Directive 5215.1. In September 1984, National Security Decision Directive 145 (NSDD 145) expanded these responsibilities to include all Federal Government agencies. As a result, the Center became known as the National Computer Security Center (NCSC) in August 1985.

The primary goal of the NCSC is to encourage the widespread availability of trusted computer systems: systems that employ sufficient hardware and software integrity measures for use in the simultaneous processing of a range of sensitive or classified information. Such encouragement is brought about by evaluating the technical protection capabilities of industry and government-developed systems, advising system developers and managers of their systems' suitability for use in processing sensitive information, and assisting in the incorporation of computer security requirements in the systems acquisition process.

The NCSC Computer Security Sub-system Evaluation Program

While the NCSC devotes much of its resources to encouraging the production and use of large-scale, multi-purpose trusted computer systems, there is a recognized need for guidance on, and evaluation of, computer security products that do not meet all of the feature, architecture, or assurance requirements of any one security class or level of the Criteria. The NCSC has, therefore, established a Computer Security Sub-system Evaluation Program.

The goal of the NCSC's Computer Security Sub-system Evaluation Program is to provide computer installation managers with information on sub-systems that would be helpful in providing immediate computer security improvements to existing installations.

Introduction

Sub-systems considered in the program are special-purpose products that can be added to existing computer systems to increase some aspect of security and have the potential of meeting the needs of both civilian and government departments and agencies. For the most part, the scope of a computer security sub-system evaluation is limited to consideration of the sub-system itself, and does not address or attempt to rate the overall security of the processing environment. To promote consistency in evaluations, an attempt is made, where appropriate, to assess a sub-system's security-relevant performance in light of applicable standards and features outlined in the Criteria. Additionally, the evaluation team reviews the vendor's claims and documentation for obvious flaws which would violate the product's security features, and verifies, through functional testing, that the product performs as advertised. Upon completion, a summary of the evaluation report is placed on the Evaluated Products List.

The report does not assign a specific rating to the product, but provides an assessment of the product's effectiveness and usefulness in increasing computer security.

PRODUCT EVALUATION

Product Overview

The Sentinel Security System is a microcomputer software hardware product capable of providing access control to programs and files (discretionary access control), user logon procedures (identification and authentication), and auditing of user actions (audit). In addition to these security features, Sentinel also prevents unauthorized attempts to format the non-removable hard disk, and has the ability to encrypt programs and files (protected objects).

The Sentinel system consists of a plug-in card which occupies an IBM PC, PC/XT, PC/AT or BIOS compatible microcomputer expansion slot, and support software. Firmware on the card monitors the bus and arbitrates accesses to protected objects, authenticates users, and performs audit. The card also has non-volatile memory which contains an audit log, and the users' passwords and access rights. Sentinel's software provides the basic utility and System Administrator management functions for the system. The functions include the assignment of access rights and passwords, and the modification of user menus.

Evaluation of Functionality

Identification and Authentication

Access to a microcomputer secured with Sentinel is controlled by requiring users to enter a valid password. There is a maximum of twenty users. Valid passwords are case-sensitive and consist of six to eight alpha-numeric characters. Sentinel allows five illegal access attempts, after which an audible alarm is sounded, the system is put into a locked condition, and a re-boot is required.

Passwords are initially assigned by the System Administrator (SA). Subsequent passwords may then be assigned by the SA, or changed by the individual users. Passwords are stored in encrypted form in non-volatile memory on the Sentinel board. The SA also has the ability to preset a lifetime, measured in days, of usage for a password.

Discretionary Access Control

Subjects in the Sentinel system are users, and the protected objects are file groups, up to a maximum of 64, and departments, up to a maximum of eight. File groups are a collection of files and programs. Files and programs are, therefore, not protected individually, but assigned to a protected file group. Departments are a collection of file groups, and are provided in order to simplify the assignment of access rights.

Sentinel implements discretionary access control between subjects and objects using user profiles. User profiles are per-user lists of file groups that a user may access, and the permitted mode of access. The SA is authorized to initially assign and change accesses to the file groups for users. One or more users may be assigned access to a file group.

Unless a user has an access right to a file group, or to the department to which that file group is assigned, no access is allowed. The access rights for file groups are read, write (includes read), and null. The access rights for departments are read and write, and are only referenced when a user attempts to access a file group to which a user has no file group access assigned. Write access allows users to move files to and from, and create files in, file groups. Read access only allows users to read and copy files from file groups. Users can assign data to file groups with individual access to protect their own data, or with multi-user access, to allow resource sharing. The access rights of a user to file groups and departments are always used in access control decisions to enforce discretionary access control.

Default protection is provided if the SA has activated the constant protection option for the system or for a particular user. While functioning in the system under this option, one of a user's file groups is a default; anything created or copied is assigned to this protected file group. If the protection option is not selected, files created or copied are unprotected, and available to any user of the system.

Users' current access authorizations for file groups and departments are stored, in encrypted form, on the Sentinel board as user profiles. Sentinel provides a management utility for the SA to modify these profiles.

The Sentinel system utilizes an optional menu system to automate the microcomputer environment. This allows the SA to isolate the users from the DOS shell, thus detering the circumvention of the discretionary access control mechanism. Non-privileged users can

therefore only access and execute objects through the use of the system-provided menus. That is, unless granted access to the DOS system functions, a user is only able to execute the menu-listed programs, e.g., application programs. The SA is the only user authorized to modify these menus to provide non-privileged users with different capabilities.

Audit

Sentinel provides optional audit capabilities which may be employed to monitor the access to the protected microcomputer, and user accesses to Sentinel protected data. The data included in the log is the time of logon/logoff, the user number, all file accesses, illegal accesses to files, and changes to passwords. Since Sentinel does not protect data to the granularity of a single file, the file group number is logged as reference of a legal or illegal access attempt.

The audit information may be viewed on-line, or in hardcopy. Sentinel provides audit display tools to analyze the data in various formats. The tools can be used to prepare reports based on user names or projects. The tools also provide a convenient means of tracking users' system utilization.

The audit log is stored in non-volatile memory on the Sentinel board. When this log becomes full, the system will either halt and wait for supervisor intervention, or continue logging, erasing earlier entries. This depends on which option has been selected by the System Administrator.

Evaluation of Documentation

The Sentinel Security System package provides three manuals, the Installation Manual, the User Manual, and the Administrator Manual, which together describe the system.

The Installation Manual is addressed to the System Administrator. The manual provides guidance on the installation and removal of the Sentinel security board and software, system hardware requirements, and information on setting up mutiple microcomputer's secured with the Sentinel system. This manual was found to accurately describe the procedures necessary to correctly install Sentinel.

Product Evaluation

The User Manual is intended for the general user. This manual provides the information needed on the protection features of Sentinel, and guidelines on their use. The manual includes proper procedures for logon, logoff, and information on Sentinel's philosophy of file protection. However, this document does not provide sufficient detail in it's description of file protection because it only lists examples of the protection, and not a full description of the mechanism. In some instances, it assumes that the System Administrator has given users a functional description of the system before reading this document.

The Administrator Manual is for the System Administrator. This document is designed to instruct the administrator on the management of the Sentinel system. The manual includes information on the security features and management utilities necessary to operate the system. This document was found in some areas to be out-of-date with the version of the system that was evaluated.

THE PRODUCT IN A TRUSTED ENVIRONMENT

The rapid introduction of office automation products into the workplace has brought with it the need to protect and control access to data created with these systems. Initially, protection was provided solely by the individuals who maintained physical possession of their own data and operating system on a floppy disk, giving a reasonably high assurance of maintaining data and code integrity. These procedural controls isolated users, and thus prevented intentional or accidental access to other users' data. Other security mechanisms were not deemed necessary since users were only able to inflict damage on their own data, or copy of the operating system.

The advent of inexpensive and reliable hard disk drives introduced new security implications. In today's working environment, it is common to have many users share and store their data on the hard disk of a shared microcomputer. In this environment, users no longer have the assurance that their data is protected from unauthorized access, or even that the underlying operating system has not been corrupted. Procedural controls can no longer provide adequate user isolation and the controlled sharing necessary for this environment.

The task of providing security on the majority of microcomputers in use today is further complicated by the fact that their architectures are primarily single-state. Single-state hardware systems can not support the more common security mechanisms found in larger, more fully integrated systems. Features such as multiple processor states (which provide for user process separation), privileged instructions (which limit user access to the trusted system processes), and memory protection (which prevents unauthorized user access to specific memory locations) are all mechanisms that help to maintain user isolation in a shared environment.

Sentinel, when configured as tested, can provide added security by requiring a user password before gaining access to the functions of the microcomputer, by controlling access to data objects by requiring assigned access, and by maintaining an audit trail that records all machine and data accesses by users. The system administrator must take certain precautions to ensure that the security mechanisms will be maintained.

The security mechanisms can be maintained only if both the operating system in which Sentinel runs, and Sentinel's operational files, are protected from unauthorized modification. Since Sentinel's protection mechanisms are implemented in

single-state machine hardware, it becomes essential that user/system separation be maintained. In order to decrease the possibility that the protection mechanisms can be circumvented, all non-privileged users must be restricted from accessing the security-relevant system functions, e.g. all DOS and direct I/O commands. This requires certain restrictions to be placed on the functionality of the system. Only the use of the application-type programs provided by the Sentinel system menus, i.e., word processors, data bases, spread sheets, etc., is allowed. The SA must ensure that the application software packages do not have 'exit to DOS' features that could be used to exit the security system, and obtain access to the system functions. Additionally, the SA must ensure the integrity of the installed application software packages. The use of compilers/assemblers for program development, or memory resident programs, should be restricted to privileged users.

The audit and access control security features are options in the Sentinel system. The SA should ensure that the system-wide options for these features are selected in order to provide default file protection, and the ability to track system activity.

The system should be configured so that the ability to change passwords is restricted to the SA. The SA is responsible for assigning a unique password to each individual user. Allowing users to change their own passwords is undesirable, because if a chosen password currently exists on the system, Sentinel notifies the user with an 'Illegal Password' message, and then prompts for another password. This message implies that the chosen password is the same as the old password, or that it already exists on the system.

PRODUCT TESTING

Testing Procedure

Testing represents a significant portion of a sub-system evaluation. The functional test suite focused upon those security features identified as being provided by the Sentinel system. Testing was intended as a functional checklist to ensure that Sentinel's audit, discretionary access control, and identification and authentication mechanisms functioned as documented. The team's testing of the discretionary access control, and identification and authentication mechanisms, involved attempts to locate flaws, but did not attempt to circumvent or subvert the Sentinel security architecture.

Product testing was performed on the following system and product configuration. The system consisted of an IBM PC/XT running PC-DOS 3.1(1), with: 512 KBytes of memory, one floppy disk drive, and an internal ten megabyte, non-removable hard drive. Sentinel was installed with the constant protection and encryption options selected, audit option selected to halt system when the log becomes full, password length set to eight characters, and password assignment restricted to the System Administrator. Special precautions were taken to ensure that non-privileged users did not have access to DOS through the menu option and menu-listed application programs.

The test plan, developed by the team, tested the discretionary access control, audit, and identification and authentication functions. The test plan consisted of establishing a list of test users, and file groups and departments. Each of the test users was assigned different access attributes to the various test file groups and departments. Files were assigned to the test file groups, and all but one were distributed on the hard drive. One file was placed on a floppy disk to test access control to file groups located on floppy disks.

Attributes were assigned so that every user had a different access to each of the file groups. There were four accesses assigned: read, write, null and no access. Each test user

---

(1) PC-DOS is a registered trademark of International Business Machines Corporation.

attempted to read and write to every test file under a protected file group. Since each test user possessed different access attributes, Sentinel was expected to deny and allow access based on the attribute. The results of the file and system access attempts, and Sentinel's user attribute tables, were compared to the events in the audit log, in order to validate the correct operation of the audit function.

Although the product provides features designed to enhance the administrative management of the system, they were not tested since they were not considered security relevant.

During the course of the testing, the team made no attempt to evaluate the strength of the data encryption scheme. The team established only that data was successfully transformed (encrypted/decrypted).

Test Results

The following is the testing results of Sentinel version 3.13, when configured as described in the Testing Procedure section, with respect to each of the evaluated security mechanisms:

Identification and Authentication

This function performed as documented; no access was allowed to the machine without first entering a valid password.

Discretionary Access Control

This mechanism performed as documented; when the precautions noted in the previous section were taken, system users were only allowed access to objects to which they had been given access. Protection was provided to the file that was located on the floppy disk.

Audit

This option performed as documented with the exception that accesses to the last file group, 64, were not logged. This is believed to be an isolated case because of a boundary condition in the code.

Even though Sentinel version 3.13, when configured as tested, placed the underlying system in an application-restricted environment with an associated reduction in functionality, the evaluation team found it provided an effective and reliable means of securing data on an IBM PC/XT.

UNCLASSIFIED
SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b. RESTRICTIVE MARKINGS NONE
2a. SECURITY CLASSIFICATION AUTHORITY	3. DISTRIBUTION / AVAILABILITY OF REPORT DISTRIBUTION UNLIMITED
2b. DECLASSIFICATION / DOWNGRADING SCHEDULE	
4. PERFORMING ORGANIZATION REPORT NUMBER(S) CSC-EPL-87/004	5. MONITORING ORGANIZATION REPORT NUMBER(S) S228,516
6a. NAME OF PERFORMING ORGANIZATION National Computer Security Center 6b. OFFICE SYMBOL (If applicable) C12	7a. NAME OF MONITORING ORGANIZATION
6c. ADDRESS (City, State, and ZIP Code) 9800 Savage Road Ft. George G. Meade, MD 20755-6000	7b. ADDRESS (City, State, and ZIP Code)
8a. NAME OF FUNDING / SPONSORING ORGANIZATION 8b. OFFICE SYMBOL (If applicable)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c. ADDRESS (City, State, and ZIP Code)	10. SOURCE OF FUNDING NUMBERS PROGRAM ELEMENT NO. / PROJECT NO. / TASK NO. / WORK UNIT ACCESSION NO

11. TITLE (Include Security Classification)

(U) Sub-system Evaluation Report, Computer Security Corp.'s Sentinel Version 3.13

12. PERSONAL AUTHOR(S)
Joseph Bulger, Leon Neufeld

13a. TYPE OF REPORT	13b. TIME COVERED	14. DATE OF REPORT (Year, Month, Day)	15. PAGE COUNT
Final	FROM _____ TO _____	870713	19

16. SUPPLEMENTARY NOTATION

17. COSATI CODES			18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB-GROUP	NCSC TCSEC sub-system Sentinel Security System Computer Security Corporation

19. ABSTRACT (Continue on reverse if necessary and identify by block number)

The Computer Security Corporation's, Sentinel Security System product was evaluated against the identification and authentication, discretionary access control and audit requirements detailed in the Department of Defense Trusted Computer System Evaluation Criteria, dated December 1985. Sentinel is a hardware/software product which, when properly installed, provides trust through the implementation of the security features listed above. This report documents the evaluation of this product.

20. DISTRIBUTION / AVAILABILITY OF ABSTRACT	21. ABSTRACT SECURITY CLASSIFICATION
☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT. ☐ DTIC USERS	UNCLASSIFIED

22a. NAME OF RESPONSIBLE INDIVIDUAL	22b. TELEPHONE (Include Area Code)	22c. OFFICE SYMBOL
LTC Lloyd D. Gary, USA	(301) 859-4458	C/C12

DD Form 1473, JUN 86 *Previous editions are obsolete.*

SECURITY CLASSIFICATION OF THIS PAGE
UNCLASSIFIED

☆U.S. Government Printing Office : 1989 - 620-016/00867